Hubert Dębniak, Stanisław Rabczuk

WYBRANE ASPEKTY PRAWNE POZYSKIWANIA DANYCH Z MEDIÓW SPOŁECZNOŚCIOWYCH PRZEZ POLSKIE ORGANY ŚCIGANIA[1]

Obtaining data from social media by Polish law enforcement agencies – selected aspects

Wprowadzenie

Na koniec 2018 roku z Internetu korzystało 28 milionów mieszkańców Polski[2], podczas gdy liczba użytkowników na całym świecie wyniosła łącznie 4,4 miliarda[3]. Z kolei liczba użytkowników mediów społecznościowych (ang. *social media*) wyniosła w Polsce 18 milionów[4], na świecie zaś – 3,5 miliarda osób[5]. Z danych dotyczących samego Facebooka wynika, że rokroczny wzrost liczby jego użytkowników w okresie 2017–2018 osiągnął w Polsce około 8%[6], na świecie zaś 9%[7]. Zwiększonemu wykorzystaniu Internetu towarzyszy wzrost

---

[1] Artykuł powstał w wyniku realizacji projektu badawczego pt. *Media społecznościowe w pracy organów ścigania* o nr. 2018/31/B/HS5/01876 kierowanego przez dr. hab. Pawła Waszkiewicza, finansowanego ze środków Narodowego Centrum Nauki. W pracach tego etapu projektu uczestniczyli: Katarzyna Bayer, Jan Bitner, Marta Czekalska, Hubert Dębniak, Karolina Fabrycka, Dominika Hoinca, Aleksandra Jędrzejak, Paulina Kargul, Kinga Krawczyk, Karolina Mazur, Michał Mazur, Stanisław Rabczuk, Karolina Skraba, Ignacy Strzałkowski, Paweł Wasylkowski. Jeżeli nie wskazano inaczej, odniesienia w artykule dotyczące badań nad wykorzystaniem mediów społecznościowych w organach ścigania dotyczą przedmiotowego projektu badawczego.

[2] *Polski internet w grudniu 2018*, Raport Gemius/PBI, online: http://pbi.org.pl/badanie-gemius-pbi/polski-internet-w-grudniu-2018/ [dostęp: 3.08.2019].

[3] *Digital 2019. Essential insights into how people around the world use the internet, mobile devices, social media, and e-commerce*, online: https://wearesocial.com/global-digital-report-2019 [dostęp: 22.07.2019].

[4] *Digital 2019 Poland. All the data and trends you need to understand internet, social media, mobile and e-commerce behaviors in 2019*, online: https://datareportal.com/reports/digital-2019-poland [dostęp: 4.08.2019].

[5] *Digital 2019…*, op. cit., zob. także *Facebook Reports Fourth Quarter and Full Year 2018 Results*, online: https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Release.pdf [dostęp: 3.08.2019]. Facebook wskazuje tam, że na koniec 2018 roku posiadał 2,32 miliarda użytkowników aktywnych miesięcznie oraz 1,52 miliarda użytkowników aktywnych dziennie.

[6] P. Rosa, *Social Media*, w: *Raport strategiczny. Internet 2018/2019*, IAB Polska, s. 54–55, online: https://iab.org.pl/wp-content/uploads/2019/06/HBRP-raport-IAB-05-191.pdf [dostęp: 22.07.2019].

[7] *Facebook Reports Fourth Quarter and Full Year 2018 Results*, op. cit.

liczby przestępstw popełnianych za jego pośrednictwem. Według danych Policji w 2018 roku w Polsce za pomocą sieci popełniono ponad 80 tysięcy przestępstw[8]. Nieznana jest jednak liczba przestępstw popełnianych wyłącznie z wykorzystaniem mediów społecznościowych. Statystyki zagraniczne wskazują na dużą dynamikę tego typu przestępczości – w Stanach Zjednoczonych według danych Federalnego Biura Śledczego (ang. Federal Bureau of Investigation, FBI) w 2017 roku było to ponad 20 tysięcy przypadków[9], przy czym liczba ta w latach 2015–2017 wzrosła trzykrotnie[10].

Organy ścigania w celu zwalczania przestępczości mogą zarówno wykorzystywać zasoby dostępne w Internecie – stosując wywiad jawnoźródłowy[11], jak i zwracać się do usługodawców z żądaniem udostępnienia informacji. Eksploracyjne badania przeprowadzone na Uniwersytecie Warszawskim[12] wskazują, że funkcjonariusze Policji wykorzystują media społecznościowe jako źródło informacji zarówno w toku czynności operacyjno-rozpoznawczych, jak i czynności śledczych oraz procesowych.

Mając na względzie złożoną problematykę prawną pozyskiwania oraz wykorzystywania tego typu danych w procesie karnym, w niniejszym artykule autorzy skupili się wyłącznie na podstawach ich pozyskiwania przez polskie organy ścigania, zawężając przedmiot pracy do wybranych mediów społecznościowych – Facebooka, Twittera oraz Instagrama[13] – i odnosząc się do danych pochodzących wyłącznie z terenu Unii Europejskiej.

Przetwarzanie danych przez serwisy społecznościowe

Z serwisów społecznościowych można korzystać zarówno w ramach wolnego dostępu[14], jak i dopiero po uprzedniej rejestracji i zalogowaniu. Jakkolwiek zalogowanie często warunkuje ujawnienie pewnych treści, to dane inter-

---

8 Dane uzyskane od Komendy Głównej Policji na podstawie wniosku o udostępnienie informacji publicznej, sierpień 2019, sygn. Gip-3099/19.

9 *FBI (2015–2017) Internet Crime Report* za: M. McGuire, *Social Media Platforms and the Cybercrime Economy*, s. 8, online: https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf [dostęp: 4.08.2019].

10 Ibidem.

11 Jako wywiad jawnoźródłowy określa się działania obejmujące proces zbierania oraz analizy informacji pochodzących ze źródeł otwartych, tj. dostępnych publicznie. W piśmiennictwie wskazuje się, że informacja jawnoźrodłowa to „ciąg danych, które pochodzą z jednego bądź większej liczby źródeł jawnych, a który to ciąg podlega procesowi oceny z uwzględnieniem ich zawartości oraz czasu publikacji" (K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011, s. 51).

12 Badania własne, zob. przypis nr 1.

13 Są to trzy najpopularniejsze w Polsce media społecznościowe po YouTube, zob. *Digital 2019 Poland…*, op. cit.

14 Korzystanie w ramach wolnego dostępu oznacza możliwość przeglądania treści znajdujących się na danym portalu bez zalogowania.

nautów przetwarzane są przez serwisy społecznościowe w każdym z wyżej wymienionych przypadków – różnicą pozostaje jedynie ich zakres.

Będąc zarówno zarejestrowanym, jak i niezarejestrowanym użytkownikiem, podczas przeglądania treści znajdujących się na stronach internetowych zostawiamy za sobą tzw. cyfrowy ślad[15]. Przez pewien czas znajduje się on zarówno na urządzeniu, z którego korzystamy (zwanym urządzeniem końcowym), infrastrukturze pośredniczącej (np. router Wi-Fi), jak i u samych usługodawców oraz ich partnerów (dostawcy usług internetowych, strony internetowe, reklamodawcy). Przeważnie dane stanowiące cyfrowy ślad spełniają definicję danych osobowych, tj. są informacją o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[16]). Korzystając z sieci, pośrednio zostawiamy także ślady cyfrowe niebędące danymi osobowymi. Są to informacje istotne dla celów biznesowych lub społecznych (np. utrzymania infrastruktury, tworzenia nowych usług, optymalizacji istniejących[17]), które nie umożliwiają bezpośredniej lub pośredniej identyfikacji danej osoby. Przykładem danych nieosobowych są dane generowane przez maszyny czy informacje dotyczące przeglądanych stron internetowych, a także dane spseudonimizowane[18]. Ramy prawne dla przetwarzania danych osobowych i nieosobowych stanowią odpowiednio RODO oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych

15 W. Kasprzak definiuje ślad cyfrowy jako zmianę w kodzie binarnym systemu teleinformatycznego, a także urządzenia cyfrowego zdolnego do przetwarzania, wysyłania, gromadzenia pakietów danych, będącą wynikiem ingerencji zewnętrznej (fizycznej) bądź wewnętrznej (zdalnej), przy czym zaznacza, że system teleinformatyczny należy rozumieć jako sieci informatyczne i ich elementy składowe – zob. W. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015, s. 25–26.

16 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (OJ L 119, 4.5.2016, p. 1–88), dalej zwane „RODO".

17 Zob. B. McKenna, *EU regulation set to advance single market for non-personal data*, „Computer Weekly", listopad 2018, online: https://www.computerweekly.com/news/252452332/EU-regulation-set-to-advance-single-market-for-non-personal-data [dostęp: 4.08.2019].

18 Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi oraz organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 5 RODO), za: K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, System Informacji Prawnej Legalis.

w Unii Europejskiej. Aktem prawnym składającym się na swobodę przepływu danych osobowych i nieosobowych na Jednolitym Rynku Cyfrowym UE jest także opracowywane obecnie tzw. rozporządzenie ePrivacy[19], które ma na celu uregulowanie zasad przetwarzania danych pochodzących z łączności elektronicznej. Zastąpi ono obowiązującą obecnie dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej[20]. W zakresie prawodawstwa polskiego zasady przetwarzania danych określa rozdział 4 ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną[21].

Portale społecznościowe będące przedmiotem niniejszego artykułu zostały utworzone przez podmioty mające swoją siedzibę w Stanach Zjednoczonych. Dlatego istotne jest określenie, czy mają do nich zastosowanie unijne przepisy dotyczące ochrony danych osobowych. Przede wszystkim należy zauważyć, że terytorialny zakres stosowania RODO, określony w art. 3 ust. 1 RODO, obejmuje przetwarzanie danych osobowych podmiotów znajdujących się na terenie Unii Europejskiej, niezależnie od miejsca przetwarzania tych danych. Niezależnie od powyższego stronami umów z użytkownikami serwisów Facebook, Twitter oraz Instagram, pochodzącymi z terenów Unii Europejskiej[22], są spółki z siedzibą w Irlandii[23], co do których stosuje się unijne przepisy dotyczące ochrony danych osobowych (mają one status administratora danych). Ponadto podmioty prawa amerykańskiego będące bezpośrednimi właścicielami serwisów Twitter, Instagram i Facebook przystąpiły do tzw. Tarczy Prywatności[24].

---

19 Zob. COM(2017) 10 final 2017/0003(COD) – Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), online: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010 [dostęp: 27.07.2019].

20 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (OJ L 201, 31.7.2002, p. 37–47).

21 Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (tekst jedn. Dz.U. z 2019 r., poz. 123).

22 W przypadku Twittera stroną umów z użytkownikami pochodzącymi z terenów innych niż Stany Zjednoczone jest spółka z siedzibą Irlandii, zob. *Twitter Terms of Service*, online: https://twitter.com/tos [dostęp: 4.08.2019]. Dane użytkowników Facebooka oraz Instagrama są z zasady przetwarzane przez spółkę z siedzibą w Stanach Zjednoczonych, z wyłączeniem użytkowników z Europy, dla których właściwy jest Facebook Ireland Ltd., zob. D. Ingram, *Facebook to put 1.5bn users out of reach of new EU GDPR privacy law*, „The Irish Times", kwiecień 2018, online: https://www.irishtimes.com/business/technology/facebook-to-put-1-5bn-users-out-of-reach-of-new-eu-gdpr-privacy-law-1.3466837 [dostęp: 4.08.2019].

23 W przypadku Twittera – Twitter International Company, One Cumberland Place, Fenian Street Dublin 2, D02 AX07, Irlandia, natomiast Instagrama oraz Facebooka – Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irlandia.

24 Ang. *Privacy Shield*, pełna nazwa: *EU–U.S. Privacy Shield Framework*, zob. oficjalną stronę internetową programu: https://www.privacyshield.gov/ [dostęp: 28.07.2019].

Jest to program, w ramach którego odbywa się certyfikacja podmiotów przetwarzających dane na terenie Stanów Zjednoczonych. Spełnienie wymagań sposobu i zakresu przetwarzania danych na poziomie zapewniającym prywatność podobną jak dla danych przetwarzanych na terenie UE umożliwia transfer danych osobowych przez tzw. spółki-córki z terenu Unii Europejskiej poza teren Europejskiego Obszaru Gospodarczego[25], do Stanów Zjednoczonych. Dla podmiotów danych program „Tarcza Prywatności" oznacza ułatwienie możliwości realizacji praw wynikających z RODO, a także zapewnienie zgodności przetwarzania danych z prawem unijnym.

W unijnych przepisach ochrony danych można wyróżnić najczęściej stosowane podstawy prawne oraz rodzaje danych osobowych przetwarzanych na ich podstawie:

a) w celu wykonania umowy (art. 6 ust. 1 lit. b. RODO), tj. świadczenia na rzecz użytkownika określonej usługi. Zakres danych przetwarzanych w ramach tej podstawy jest ściśle powiązany z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO), zgodnie z którą usługodawca powinien żądać wyłącznie danych bezwzględnie niezbędnych dla świadczonych usług. Przykładowo danymi niezbędnymi do świadczenia usługi w ramach serwisu Instagram, w zakresie danych wskazywanych przez użytkownika, będą numer telefonu komórkowego lub adres email, imię i nazwisko oraz nazwa użytkownika;
b) w celu prawnie uzasadnionego interesu administratora danych (art. 6 ust. 1 lit. f RODO), tj. stosowania marketingu własnych usług/produktów, zapobiegania oszustwom, dostosowywania treści, analizowania aktywności użytkowników, dochodzenia praw lub obrony przed roszczeniami – przy czym podstawa ta nie powinna być stosowana w stosunku do dzieci[26];
c) w celach, na które podmiot danych wyraził zgodę (art. 6 ust. 1 lit. a RODO), np.: przetwarzania danych do celów marketingowych przez osoby trzecie, w tym przetwarzania zautomatyzowanego (profilowanie) celem oferowania dopasowanych informacji marketingowych, przetwarzania podanych przez użytkownika danych, które nie były niezbędne do świadczenia usługi, prowadzenia badań rynku.

---

[25] Obecnie członkami Europejskiego Obszaru Gospodarczego (EOG) są państwa członkowskie Unii Europejskiej oraz Islandia, Norwegia i Liechtenstein, zob. *Agreement on the European Economic Area*, https://www.efta.int/sites/default/files/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf [dostęp: 6.08.2019].

[26] Zakaz stosowania podstawy prawnie uzasadnionego interesu administratora w przypadku danych osobowych dzieci wynika z wykładni językowej art. 6 ust. 1 lit. f RODO – zob. P. Litwiński, P. Barta, M. Kawecki, *Artykuł 6 RODO*, nb 58, w: P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, System Informacji Prawnej Legalis.

Szczególne zasady przetwarzania danych odnoszą się do tzw. danych osobowych wrażliwych (art. 9 RODO), tj. danych dotyczących zdrowia, seksualności, poglądów politycznych, pochodzenia rasowego lub etnicznego czy danych biometrycznych. Przetwarzanie takich danych jest możliwe przez administratora m.in. w przypadku wyrażenia wyraźnej zgody czy upublicznienia w sposób oczywisty tych danych. Upublicznienie może nastąpić wyłącznie przez podmiot danych lub przez inną osobę za jego wyraźną zgodą, jeżeli upublicznienie zostało dokonane wobec nieoznaczonego grona adresatów[27]. W piśmiennictwie wskazuje się, że kryterium podania danych do publicznej wiadomości spełnia podanie danych na ogólnie dostępnych forach internetowych czy grupach dyskusyjnych, nawet jeśli wymagają one logowania[28]. Stąd dane podawane na portalach społecznościowych, zwłaszcza gdy oznaczane są jako dostępne publicznie, dla określonego obszaru lub dla znajomych podmiotu danych, mogą być uznawane za upublicznione dla nieoznaczonego kręgu adresatów, a stąd przetwarzane przez administratora na podstawie art. 9 ust. 2 lit. e RODO.

Dane podlegające szczególnej ochronie mogą stanowić element postów, fotografii czy wiadomości prywatnych. Ponadto w przypadku Facebooka profil osoby może zostać uzupełniony o informacje na temat poglądów religijnych oraz politycznych. Wyłącznie w tym przypadku wobec użytkownika wyświetlany jest komunikat z żądaniem zaakceptowania zasad przetwarzania danych oraz ich upublicznienia. Facebook informuje użytkownika o tym, że dane wrażliwe będą przetwarzane do celów marketingowych, w tym profilowania. Jak wspomniano jednak powyżej, dane na temat chociażby seksualności mogą zostać uzyskane nie tylko z treści zamieszczonych bezpośrednio na profilu danej osoby. Całokształt aktywności podmiotu danych: polubione zdjęcia, komentarze, strony czy zaangażowanie w pewne wydarzenia, może prowadzić do poznania jego zainteresowań i poglądów[29].

---

27 Ibidem, art. 9, nb. 20.

28 Uwagi na tle starej ustawy o ochronie danych, które nie straciły na aktualności po wejściu w życie RODO, zob. P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, wyd. 4, Warszawa 2016, art. 27, nb. 23, System Informacji Prawnej Legalis.

29 Z badań przeprowadzonych w styczniu 2018 roku, tj. na kilka miesięcy przed rozpoczęciem obowiązywania RODO, wynika, że Facebook na podstawie ogólnej aktywności użytkowników profilował m.in. ich orientację seksualną – zob. J.G. Cabañas, Á. Cuevas, R. Cuevas, *Unveiling and quantifying Facebook exploitation of sensitive personal data for advertising purposes*, 2018, online: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-cabanas.pdf [dostęp: 28.07.2019]. Obecnie informacja dotycząca wykorzystania danych wrażliwych znajdująca się w *Zasadach dotyczących danych Facebooka* odnosi się do danych uzyskanych na podstawie wyraźnej zgody, a także tych, które użytkownik zdecydował się wyraźnie udostępnić.

Portale społecznościowe przetwarzają także dane niebędące tzw. danymi wrażliwymi, które pozyskują samodzielnie lub od partnerów. Nawet informacje dotyczące danej osoby niebędącej zarejestrowanym użytkownikiem mogą być przetwarzane przez portale społecznościowe, chociażby w wyniku działań innego użytkownika, który zaimportuje swoje kontakty z telefonu do serwisu lub umożliwi aplikacji społecznościowej dostęp do listy swoich połączeń telefonicznych lub wiadomości tekstowych[30]. Także reklamodawcy mogą dodawać dane osób do listy klientów, która następnie jest dopasowywana do danego profilu na Facebooku. Stąd pochodzące od osób trzecich informacje na temat podmiotu danych są przetwarzane przez portale społecznościowe, nawet gdy użytkownik nie jest zarejestrowany na platformie. Skutkiem takiego przetwarzania jest np. proponowanie nowo zarejestrowanym osobom dodania do znajomych użytkowników poznanych w rzeczywistości, jak i wyświetlanie reklam zgodnych z ich zainteresowaniami.

Głównie jednak portale społecznościowe zapełniane są treściami wytworzonymi przez użytkowników – intencjonalnie lub nieświadomie. Przykładem może być umieszczenie na Instagramie zdjęcia z wakacji. Oprócz samego obrazu wraz z dodanym przez użytkownika opisem portal społecznościowy pobiera i analizuje inne dane, jak chociażby metadane dotyczące urządzenia, którym wykonano zdjęcie, miejsca wykonania zdjęcia czy daty utworzenia przesyłanego pliku. Większość gromadzonych informacji nie jest jednak udostępniana publicznie, ale służy jedynie celom marketingowym, statystycznym lub jest wykorzystywana do rozwijania serwisu. Facebook oraz Instagram[31] uzyskują także informacje z urządzeń końcowych, otrzymując przykładowo dane: o systemie operacyjnym, przeglądarce, baterii, sile sygnału, zainstalowanych wtyczkach, ruchach myszy, informacji, czy strona jest otwarta na pierwszym planie lub w tle, identyfikatorach urządzeń – adresach MAC (ang. *Media Access Control adress*)[32], adresie IP (ang. *IP adress*)[33], identyfikatorach reklamowych, w tym *ID cookies*[34], liście punktów dostępu wi-fi, nadajnikach sieci komórko-

[30] Zob. *Zasady dotyczące danych Facebooka*, online: https://www.facebook.com/policy.php [dostęp: 28.07.2019].

[31] Podobny zakres danych jest zbierany przez Twittera, zob. *Twitter Privacy Policy*, online: https://twitter.com/en/privacy [dostęp: 28.07.2019].

[32] Adres MAC jest unikatowym adresem karty sieciowej, nadawanym przez producenta w trakcie produkcji. Zob. M. Cunche, *I know your MAC Address: Targeted tracking of individual using Wi-Fi*, online: https://hal.inria.fr/file/index/docid/858324/filename/Wi-Fi_Stalking.pdf [dostęp: 6.08.2019].

[33] Adres IP jest niepowtarzalnym w danej chwili adresem nadawanym indywidualnie każdemu urządzeniu podłączonemu do internetu. Adres ten może się wielokrotnie zmieniać dla jednego urządzenia, albowiem jest on co do zasady stały tylko na czas danego połączenia. Zob. T. Fołta, A. Mucha, *Zniesławienie i znieważenie w internecie*, „Prokuratura i Prawo" 2006, nr 11, s. 55–56.

[34] *ID Cookie* jest trwałym identyfikatorem danego ciasteczka (ang. *cookie*), czyli pliku teksto-

wych znajdujących się w pobliżu, nazwie operatora sieci lub dostawcy Internetu, języku, strefie czasowej, numerze telefonu komórkowego oraz innych danych udostępnianych za zgodą użytkownika – np. lokalizacji GPS[35]. Niektóre z wyżej wymienionych informacji mogą być przesyłane nie tylko, gdy użytkownik korzysta bezpośrednio z portalu społecznościowego, ale także gdy znajduje się na innych stronach internetowych lub aplikacjach, które wykorzystują interfejs programistyczny aplikacji (ang. *application programming interface*, API)[36] danego portalu[37].

Zakres danych przetwarzanych przez portale społecznościowe jest bardzo szeroki, niemniej wszystkie dane podlegają retencji, której okres zależny jest od ich rodzaju. Z informacji podawanych przez samych usługodawców wynika, że przykładowo historia wyszukiwania, nawet gdy zostanie usunięta z poziomu użytkownika, jest przechowywana przez Facebooka przez okres sześciu miesięcy, kopia dowodu tożsamości zaś, wykorzystywana przy weryfikacji konta, usuwana jest po trzydziestu dniach[38].

Niewątpliwie serwisy społecznościowe posiadają kompleksowy i szeroko rozbudowany system zbierania oraz przetwarzania informacji o użytkownikach. Podstawowym celem zbierania danych jest świadczenie usług oraz dostarczanie dopasowanych reklam. Niemniej, jak każdy usługodawca, także portale społecznościowe zobowiązane są współdziałać z organami ścigania oraz wymiaru sprawiedliwości w przypadkach przewidzianych właściwymi przepisami.

Pozyskiwanie danych przez organy ścigania

Wprowadzenie

Organy ścigania w celu pozyskiwania danych z portalów społecznościowych mogą wykorzystywać zarówno biały wywiad, jak i korzystać z uprawnień śledczych, kierując do usługodawców żądania udostępnienia danych. Samo pojęcie białego wywiadu nie jest w żaden sposób uregulowane przez prawo

wego zapisywanego na urządzeniu użytkownika przez przeglądarkę internetową na żądanie strony internetowej, przesyłaną do danego serwera za każdym razem, kiedy odwiedzana jest ponownie witryna sieciowa. Zob. A. Klein, B. Pinkas, *DNS cache-based user tracking*, online: https://www.ndss-symposium.org/wpcontent/uploads/2019/02/ndss2019_04B-4_Klein_paper.pdf [dostęp: 6.08.2019].

35 *Zasady dotyczące danych…*, op. cit.

36 Zob. *What is an API?*, online: https://www.mulesoft.com/resources/api/what-is-an-api [dostęp: 4.08.2019].

37 Zob. D. Baser, *Hard questions: What data does Facebook collect when I'm not using Facebook, and why?*, Facebook Newsroom, kwiecień 2018, online: https://newsroom.fb.com/news/2018/04/data-off-facebook/ [dostęp: 4.08.2019].

38 *Zasady dotyczące danych…*, op. cit.

polskie, zatem przy jego definiowaniu należy korzystać z dorobku doktryny[39]. Jedną z propozycji przedstawia Krzysztof Mroziewicz, który określa biały wywiad jako analizę informacji z legalnie dostępnych źródeł[40]. Dane pozyskiwane w ten sposób z mediów społecznościowych cechują się otwartą dostępnością dla użytkowników portalu, a nawet osób, które tymi użytkownikami nie są, tj. uzyskują dostęp do pewnych danych, mimo że nie są zalogowane. Dostęp do przedmiotowych danych może być jednak ograniczony, na przykład przez zawężenie dostępu do zawartych tam treści tylko dla zarejestrowanych użytkowników. Ten sposób pozyskiwania danych przez organy ścigania nie wymaga zwrócenia się z wnioskiem o ich udostępnienie do samego usługodawcy, ponieważ są one już ujawnione z zasady przez samego użytkownika danego portalu.

Niezależnie od możliwości skorzystania z dostępu do źródeł otwartych organy ścigania mogą nawiązywać współpracę z usługodawcami bezpośrednio albo wykorzystując w tym celu instrumenty międzynarodowej pomocy prawnej[41]. W tym przypadku organy ścigania zwracają się z prośbą do usługodawcy, który prowadzi portal społecznościowy, o udostępnienie konkretnych danych użytkownika. Zwrotnie przekazane informacje przeważnie zawierają dane niemające charakteru publicznie dostępnego – przykładowo są to dane adresu IP rejestracji użytkownika, numeru telefonu, adresu poczty elektronicznej czy dane lokalizacyjne[42].

Uzyskiwanie informacji jawnoźródłowych z mediów społecznościowych

W trakcie badań nad problematyką wykorzystania mediów społecznościowych w pracy organów ścigania respondenci wyrażali różnorodne opinie co do kwalifikacji prawnej czynności białowywiadowczych dokonywanych w zakresie mediów społecznościowych[43]. Uczestniczący w badaniach funkcjonariusze Policji podejmowali próby ich ujęcia jako czynności operacyjno-rozpoznawczych albo czynności procesowych. Rozróżnienie to jest doniosłe praktycznie, chociażby ze względu na odmienne reżimy dokumentowania oraz dostępu do gromadzonych informacji w toku wykonywania tych czynności.

---

[39] Zob. B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 148.

[40] K. Mroziewicz, *Czas pluskiew*, Wydawnictwo Sensacje XX Wieku Bogusław Wołoszański, Warszawa 2007, s. 334, za: K. Jarczewska-Walendziak, *Wykorzystywanie otwartych źródeł informacji przez służby śledcze*, „Toruńskie Studia Bibliologiczne" 2017, nr 1 (18), s. 137. Zob. także propozycje przedstawione przez innych przedstawicieli doktryny, przywołane w: B. Stromczyński, P. Waszkiewicz, op. cit.

[41] Badania własne, zob. przypis nr 1.

[42] *Informacje dla organów ścigania*, online: https://www.facebook.com/safety/groups/law/guidelines/ [dostęp: 4.08.2019].

[43] Badania własne, zob. przypis nr 1.

Wspomniane wcześniej wątpliwości funkcjonariuszy Policji w zakresie ujmowania czynności białowywiadowczych jako czynności operacyjnych lub procesowych nie są odosobnione, albowiem przeprowadzone w Polsce badania Jędrzeja Pogorzelskiego wskazują na istnienie tożsamego dylematu wśród prokuratorów[44].

Podstawą do stosowania czynności operacyjno-rozpoznawczych przez Policję jest art. 14 ust. 1 ustawy o Policji[45]. Termin ten pojawia się również w innych ustawach regulujących działania służb, na przykład w ustawie o Agencji Bezpieczeństwa Wewnętrznegoi Agencji Wywiadu[46] oraz ustawie o Centralnym Biurze Antykorupcyjnym[47]. Brak jest natomiast w polskim prawodawstwie definicji tych czynności[48]. Szczątkowe regulacje obejmują co najwyżej konkretne przykłady czynności operacyjno-rozpoznawczych, z wymienionymi przesłankami ich stosowania[49]. Próbę zdefiniowania tego pojęcia podjęli autorzy projektu ustawy o czynnościach operacyjno-rozpoznawczych z 2008 roku[50], która jednak nigdy nie weszła w życie. Również w literaturze przedmiotu podejmowane były próby zdefiniowana tych czynności i za trafne należy uznać stanowisko Tadeusza Hanauska, którego zdaniem „czynności operacyjne stanowią odrębny system poufnych lub tajnych działań organów policyjnych, prowadzonych poza procesem karnym, przy czym czynności te służą aktualnym lub przyszłym celom tego procesu"[51]. W świetle ustawy o Policji jednym

---

44 Prawie 60% badanych prokuratorów uznało pozyskiwanie i analizowania źródeł otwartych za czynności operacyjno-rozpoznawcze, zob. J. Pogorzelski, *Wykorzystanie otwartych źródeł informacji w pracy prokuratora*, w: W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Wydawnictwo C.H. Beck, Warszawa 2012, s. 156.

45 W granicach swych zadań Policja w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń wykonuje czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe (Ustawa z dnia 6 kwietnia 1990 roku o Policji, tekst jedn. Dz.U. z 2019 r., poz. 161), w tym zakresie zob. także: M. Rogacka-Rzewnicka, P. Girdwoyń, *Undercover Operation, Rapports Polonais XIXth International Congress Of Comparative Law Vienne 20–26 VII 2014*, Łódź 2014, s. 381.

46 Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz.U. z 2018 r., poz. 2387).

47 Ustawa z dnia 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz.U. 2018, poz. 2104).

48 T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, wyd. IX, Wolters Kluwer, Warszawa 2014, s. 624.

49 Por. art. 19 oraz 19a ustawy o Policji.

50 Zob. art. 2 oraz art. 3 Projektu ustawy o czynnościach operacyjno-rozpoznawczych, online: http://orka.sejm.gov.pl/proc6.nsf/projekty/353_p.htm [dostęp: 29.07.2019].

51 T. Hanausek, *Kryminalistyka. Zarys wykładu*, Zakamycze, Kraków 1996, s. 96. Zob. także definicję J. Krwawicza, którego zdaniem praca operacyjna to system zbierania, w zasadzie w drodze czynności pozaprocesowych, informacji niezbędnych do ustalenia zamiarów oraz działalności przestępcy, jak również ujawnienia nieznanych policji przestępstw lub uzupeł-

z celów stosowania czynności operacyjno-rozpoznawczych jest rozpoznawanie przestępstw i wykroczeń, w tym rozmiaru ich występowania, formy, jaką one przybierają, oraz prawdopodobieństwa ich wystąpienia[52].

Media społecznościowe mogą stanowić źródło wszelakiego rodzaju informacji, również takich, które mogą mieć znaczenie dla procesu karnego. Przykładowo użytkownik może opublikować film lub zdjęcie dokumentujące popełnienie czynu zabronionego. Ponadto samo wykorzystanie portalu społecznościowego może być elementem *modus operandi* sprawcy, chociażby przy tzw. przestępstwach z nienawiści[53]. W takich przypadkach organy ścigania, podejmując czynności w odniesieniu do mediów społecznościowych, mogą uzyskać bezpośrednie dowody popełnienia przestępstwa. Media społecznościowe mogą jednak zostać wykorzystane także do innych celów, takich jak chociażby ustalenie powiązań osobowych sprawcy. Tego typu działania, w świetle przywołanych wcześniej definicji, mogą zostać uznane za czynności operacyjno-rozpoznawcze, co może wywoływać wątpliwości ze względu na zróżnicowane uregulowanie tej problematyki w ustawach dotyczących ABW, AW oraz CBA.

Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu przewiduje podział na czynności operacyjno-rozpoznawcze i analityczno-informacyjne, co zdaniem Błażeja Stromczyńskiego oraz Pawła Waszkiewicza może wskazywać na rozróżnienie między białym wywiadem a czynnościami operacyjno-rozpoznawczymi[54]. Ich stanowisko opiera się jednak na brzmieniu art. 20 ustawy o Policji sprzed nowelizacji[55]. Wskazywano w niej, że Policja może pozyskiwać informacje, w tym informacje niejawne, co miałoby wskazywać, że z reguły informacje powinny być uzyskiwane jawnie. Niezależnie od powyższego, przy założeniu jawności tych działań, w świetle cytowanej definicji T. Hanauska czynności te nie mogłyby być uznawane za czynności operacyjno-rozpoznawcze z uwagi na utratę przymiotu tajności. Należy jednak wskazać, że w obecnym stanie prawnym Policja w realizacji swoich zadań ustawowych uprawniona jest do „przetwarzania informacji, w tym danych oso-

niania wiadomości o przestępstwach znanych, za: T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, op. cit., s. 624.

52 Zob. art. 14 ustawy o Policji.

53 Zob. wywiad z Rzecznikiem Praw Obywatelskich Adamem Bodnarem: N. Sawka, *Ile jest przestępstw z nienawiści? Czy oficjalne dane są zaniżone?*, styczeń 2019, online: http://sonar.wyborcza.pl/sonar/7,156422,24374999,jak-mowa-nienawisci-staje-sie-elementem-naszej-codziennosci.html?disableRedirects=true [dostęp: 4.08.2019].

54 Zob. B. Stromczyński, P. Waszkiewicz, op. cit., s. 163–165. Podobnie kompetencje służb ujmuje ustawa o Centralnym Biurze Antykorupcyjnym.

55 Nowela ustawy o Policji dokonana ustawą z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

bowych”[56]. Brak jest zatem podziału sposobu pozyskania informacji na sposób jawny i niejawny. Zakładając racjonalność ustawodawcy, należy przyjąć celowość tego rozwiązania. Jeżeli ustawa o Policji nie posługuje się terminem czynności analityczno-informacyjnych, to znaczy, że w przypadku tej formacji ustawodawca nie rozróżnia tych czynności. Dlatego należy podać w wątpliwość celowość rozróżniania czynności analityczno-informacyjnych i operacyjno-rozpoznawczych w kontekście białego wywiadu prowadzonego przez funkcjonariuszy Policji.

Przykładem czynności operacyjno-rozpoznawczych Policji w mediach społecznościowych może być założenie konta na dane fikcyjne, które ma zostać wykorzystane wyłącznie do czynności służbowych. Wykorzystanie tego konta do przeglądania treści otwartych należy uznać za czynność białowywiadowczą, natomiast wysłanie zaproszenia do znajomych na Facebooku, dołączenie do zamkniętej grupy czy nawiązanie bezpośredniego kontaktu z figurantem stanowi już wyjście poza granice białego wywiadu. Dokonywanie wyżej wskazanych czynności z wykorzystaniem konta zawierającego prawdziwe dane funkcjonariusza Policji będzie stanowić czynność operacyjną, niemniej należy podkreślić, że jest to działanie niewłaściwe. Przy wykonywaniu tego typu czynności co do zasady należałoby zachować daleko posuniętą ostrożność i chronić funkcjonariusza Policji przed ujawnieniem jego danych osobowych.

Należy jednak zauważyć, że wykorzystanie kont założonych na dane fikcyjne stoi w sprzeczności z regulaminem Facebooka[57], stanowiącym część umowy między użytkownikiem portalu a usługodawcą. W przypadku gdy konto zostanie zgłoszone jako fałszywe lub usługodawca sam stwierdzi, że tożsamość użytkownika może się różnić od danych podanych przy rejestracji, Facebook może zażądać weryfikacji, która polega na przesłaniu dokumentu urzędowego. W takim przypadku funkcjonariusz Policji posiadający konto założone na dane fikcyjne może skorzystać z fałszywej tożsamości, czego podstawę stanowi art. 20a ust. 2 ustawy o Policji[58]. Doraźnym rozwiązaniem może być także założenie nowego konta, jeżeli konto poddane weryfikacji nie umoż-

[56] Art. 20 ustawy o Policji.

[57] Początkowo Facebook w swoich niejawnych wytycznych dla organów ścigania zawarł prośbę o niekorzystanie z fałszywych kont w celu prowadzenia postępowania, zob. *Facebook Law Enforcement Guidelines*, https://info.publicintelligence.net/Facebook2010-2.pdf [dostęp: 29.07.2019]. Obecnie w wytycznych Facebooka dla organów ścigania brak jest takiej prośby, zob. *Regulamin Facebooka*, online: https://pl-pl.facebook.com/legal/terms [dostęp: 29.07.2019].

[58] Przy wykonywaniu czynności operacyjno-rozpoznawczych policjanci mogą posługiwać się dokumentami publicznymi w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz.U. z 2019 r., poz. 53) lub innymi dokumentami, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza Policji oraz środków, którymi posługuje się przy wykonywaniu zadań służbowych.

liwia dostępu do szczególnych informacji, np. poprzez dostęp do zamkniętych grup.

Problem kont założonych na dane fikcyjne nie występuje w przypadku Twittera, gdzie w umowie zawieranej między użytkownikiem a usługodawcą nie ma wymogu podawania swoich prawdziwych danych[59]. Jedyna sprzeczność między postanowieniami umowy a ewentualnymi czynnościami operacyjnymi mogłaby wystąpić w związku z zakazem naśladownictwa[60]. Hipotetycznie mogłoby to utrudnić prowadzenie gry operacyjnej polegającej na podszywaniu się pod konkretną osobę.

W dostępnych publicznie źródłach prawa wewnętrznego Policji brak jest definicji białego wywiadu. Jednak wykorzystanie źródeł otwartych, w tym mediów społecznościowych, pojawia się w załącznikach do decyzji Komendanta Głównego Policji, określających programy szkoleniowe w ramach kursów specjalistycznych[61].

Wspomniane wcześniej implikacje zakwalifikowania przedmiotowych czynności jako czynności operacyjno-rozpoznawczych albo czynności procesowych są istotne praktycznie chociażby w zakresie dostępu do informacji o podjęciu tych czynności. Czynności operacyjno-rozpoznawcze charakteryzują się poufnością. Zatem informacja o ich podjęciu powinna znaleźć się wyłącznie w tzw. aktach operacyjnych Policji, do których nie mają dostępu strony postępowania karnego. Równoległe prowadzenie dokumentacji czynności operacyjno-rozpoznawczych wynika z ich charakterystyki, albowiem prowadzone są one pozaprocesowo, niejako obok procesu karnego. Dopiero gdyby w wyniku podjętej czynności udało się zdobyć istotny dowód, powinien on zostać wprowadzony do procesu z zachowaniem wymagań art. 393 § 1 Kodeksu postępowania karnego[62]. Przykładem ilustrującym wyżej wskazany proces może być czynność operacyjnego sprawdzenia aktywności na Facebooku, w wyniku której ujawniony zostanie film potwierdzający dokonanie czynu zabronionego. Dopiero przeprowadzenie oględzin tego filmu i umieszczenie właściwego protokołu w aktach sprawy stanowić będzie czynność procesową, mogącą stano-

59 *Zasady Twittera*, online: https://help.twitter.com/pl/rules-and-policies/twitter-rules [dostęp: 29.07.2019].

60 Ibidem.

61 Zob. Decyzję nr 322 Komendanta Głównego Policji z dnia 24 października 2018 r. w sprawie programu nauczania na kursie specjalistycznym w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową, w której jednym tematów kursu jest pozyskiwanie informacji ze źródeł powszechnie dostępnych. Podobnie tematyka ta występuje również w Decyzji Komendanta Głównego Policji nr 354 z dnia 13 listopada 2015 r. w sprawie programu nauczania na kursie specjalistycznym z analizy kryminalnej w zakresie cyberprzestępczości.

62 Ustawa z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego (tekst jedn. Dz.U. z 2018 r., poz. 1987, ze zm.), dalej: k.p.k.

wić podstawę rozstrzygnięcia sądu. Zewnętrzny obserwator nie będzie przy tym wiedział, jakie czynności legły u podstaw sporządzenia protokołu[63].

Pozyskiwanie danych na podstawie współpracy z usługodawcami

Wzajemne prawa i obowiązki między użytkownikiem a usługodawcą, w tym także sposób udostępniania danych użytkownika, normuje regulamin danej usługi. W pierwszej kolejności omówione zostaną zasady dotyczące Facebooka oraz Instagrama, następnie zaś Twittera.

Facebook oraz Instagram

Przede wszystkim należy zwrócić uwagę na § 4 pkt 1 Regulaminu Facebooka, który daje usługodawcy możliwość bieżącego aktualizowania regulaminu[64]. Aktualność zawartych w niniejszym artykule informacji należy zatem oceniać według regulaminu obowiązującego na dzień złożenia go do druku[65]. Pojęcie organów ścigania występuje tylko w § 1 Regulaminu Facebooka, w punkcie dotyczącym zwalczania przypadków szkodliwego działania, gdzie usługodawca wskazuje, że w razie występowania szkodliwych wobec innych użytkowników działań lub treści Facebook może podjąć odpowiednie środki, wśród których wymienione jest zawiadomienie organów ścigania. W samej treści regulaminu brak jest sprecyzowania, co może się kryć za pojęciem szkodliwych działań, niemniej pomocne w tym zakresie mogą być publikowane przez usługodawcę tzw. standardy społeczności, wyznaczające zasady aktywności w ramach serwisu.

Reguły udostępniania informacji organom ścigania opisane są w zasadach dotyczących danych, które opisują sposób, w jaki portal udostępnia dane swoich użytkowników, przy czym są one wiążące również w zakresie Instagrama, Messengera, a także innych produktów czy funkcji oferowanych przez Facebooka[66]. W tym miejscu należy podkreślić, że właścicielem portalu społecznościowego Instagram jest sam Facebook, dlatego też sposoby udostępniania danych w obu serwisach się pokrywają. Wśród informacji zawartych w przedmiotowych zasadach wskazani zostali rodzajowo partnerzy którym Facebook może udostępniać dane użytkowników. Znajdują się wśród nich między innymi reklamodawcy, badacze i naukowcy, ale, co istotne, także ograny ścigania.

63 Z uwagi na zakres tematyczny niniejszego artykułu należy jedynie zasygnalizować problematykę wprowadzania dowodów z mediów społecznościowych do procesu karnego.

64 Regulamin Facebooka.

65 Tj. zgodnie z Regulaminem Facebooka, zaktualizowanym dnia 31 lipca 2019 roku.

66 *Zasady dotyczące danych…*, op. cit.

Facebook udziela informacji organom ścigania w dwóch przypadkach – odpowiedzi na wezwania sądowe oraz wniosków o udostępnienie danych bez wezwania sądowego, czyli w tzw. trybie nagłym.

Niewątpliwie częściej stosowane jest wnioskowanie o udostępnienie danych z wykorzystaniem wezwania sądowego[67], które na gruncie polskich przepisów powinno być rozumiane jako właściwe postanowienie prokuratora. Niemniej usługodawca wymienia warunki, od których spełnienia uzależnia udzielenie tej odpowiedzi. Po pierwsze, sam usługodawca musi mieć oparte na dobrej wierze przekonanie, że istnieje taki obowiązek w świetle prawa. Po drugie, usługodawca musi mieć przekonanie, że udzielenie odpowiedzi jest wymagane przepisami danej jurysdykcji, dotyczy użytkowników z danej jurysdykcji i jest zgodne ze standardami międzynarodowymi. Tego typu warunki mogą być ustalane przez usługodawców, albowiem wykonanie danego postanowienia leży wyłącznie w zakresie ich dobrej woli wobec transgranicznego charakteru żądania i przekazania go bezpośrednio do usługodawcy, z pominięciem organów państwa siedziby danej spółki.

W drugim z omawianych trybów udostępnienia informacji usługodawca nie wymaga już wezwania sądowego. Dane udostępniane są organom ścigania w celu zapobiegania zagrożeniu życia lub zdrowia ludzkiego, tj. w przypadkach nagłych.

Niezależnie od powyższego Facebook zaznacza, że może dane na pewien czas „zamrozić"[68], o ile są one przedmiotem właściwego żądania, zgłoszonego w dowolnym z wyżej wymienionych trybów.

Sposób kontaktu i przekazywania informacji przez portal został opisany w wytycznych dla organów ścigania, które znajdują się na stronie centrum bezpieczeństwa Facebooka[69]. Portal zastrzega, że dane z kont mogą być ujawnione wyłącznie w sposób zgodny z regulaminem oraz z amerykańską ustawą federalną *Stored Communications Act* („SCA"), 18 U.S.C., sekcje 2701–2712. Jest to ustawa z 1986 roku, która ustanawia ramy prawne udostępnienia komunikacji elektronicznej upoważnionym podmiotom w Stanach Zjednoczonych[70]. Wymagania stawiane organom ścigania są różne, w zależności od tego, jaki

---

67 W raporcie za okres lipiec–grudzień 2018 roku tylko 188 wezwań do Facebooka zostało skierowanych w tzw. trybie pilnym, w stosunku do 1912 żądań ogółem, zob. *Facebook Transparency Report – Poland*, online: https://transparency.facebook.com/government-data-requests/country/PL [dostęp: 4.08.2019].

68 Tzn. zabezpieczyć dane przed zmianami, w tym przed usunięciem, bez ich udostępniania.

69 Zob. *Informacje dla organów ścigania*, op. cit.

70 A. Golański, *Sukces Microsoftu w walce z wujem Samem: serwery w Europie poza jurysdykcją USA*, lipiec 2016, online: https://www.dobreprogramy.pl/Sukces-Microsoftu-w-walce-z-wujem-Samem-serwery-w-Europie-poza-jurysdykcja-USA,News,74797.html [dostęp: 4.08.2019].

jest przedmiot żądania. We wniosku o ujawnienie podstawowych danych użytkownika powinno zostać zawarte wezwanie sądowe wystawione w związku z toczącym się postępowaniem karnym. Musi ono zawierać następujące dane, o ile są dostępne: imię i nazwisko osoby, której dane są żądane, czas korzystania z serwisu, dane kart kredytowych, adresy mailowe i adresy IP, z których po raz ostatni logowano się i wylogowywano[71]. Do ujawnienia niektórych danych i innych informacji dotyczących konta, wyjąwszy treści komunikacji, obejmujących nagłówki wiadomości czy adresy IP, wymagany jest nakaz sądowy zgodny z postanowieniami 18 U.S.C., sekcją 2703(d) wspominanej ustawy. Norma wymienionego przepisu wymaga, żeby nakaz sądowy określał konkretne fakty uzasadniające, że przedmiotowe informacje będą miały znaczenie dla toczącego się postępowania karnego[72]. Do ujawnienia zapisanej zawartości konta, obejmującej na przykład wiadomości, zdjęcia, filmy, posty na osi czasu i informacje o lokalizacji, wymagany jest nakaz rewizji mający uzasadnione podstawy, zgodnie z federalnymi zasadami postępowania w sprawach karnych (ang. *Federal Rules of Criminal Procedure*) lub odpowiadającymi im procedurami stanowymi[73].

Podstawy prawne wskazywane przez Facebooka, a także tworzone przez niego procedury dobrowolnej współpracy z organami ścigania, mogą opierać się na przepisach amerykańskich, albowiem jest to jedynie fakultatywny sposób udostępnienia danych organom ścigania. Dopiero w przypadku skierowania wniosku w ramach pomocy prawnej należy oprzeć się na właściwych przepisach prawa międzynarodowego oraz lokalnego właściwych usługodawcy.

W swoich wytycznych Facebook wymienia dwa sposoby nawiązania kontaktu w celu złożenia prośby o udostępnienie danych w ramach trybu dobrowolnego udostępnienia danych. Pierwszym jest internetowy system obsługi organów ścigania, przeznaczony tylko dla funkcjonariuszy posiadających adres mailowy z domeną rządową „gov”[74]. Drugim – składanie próśb za pomocą korespondencji tradycyjnej na irlandzki adres siedziby spółki.

Na podstawie relacji jednego z funkcjonariuszy uzyskanej w toku przeprowadzonych badań[75] można wywieść, jak w praktyce polskich organów ścigania wygląda pierwsza ze wspomnianych wyżej procedur. Po weryfikacji przez usługodawcę, że żądanie pochodzi od uprawnionego funkcjonariusza,

71 *Informacje dla organów ścigania*, op. cit.

72 *18 U.S. Code § 2703. Required disclosure of customer communications or records*, online: https://www.law.cornell.edu/uscode/text/18/2703 [dostęp: 4.08.2019].

73 *Informacje dla organów ścigania*, op. cit.

74 Zob. *Law Enforcement Online Requests*, online: https://www.facebook.com/records/login/ [dostęp: 4.08.2019].

75 Badania własne, zob. przypis nr 1.

istnieje możliwość wysłania zgłoszenia udostępnienia danych, do którego należy dołączyć odpowiednie postanowienie prokuratorskie, zawierające dokładne określenie profilu, treści naruszającej prawo, a także ewentualnie zrzuty ekranu (ang. *print screen*). Zgłoszenie ma nadawany numer i jest rejestrowane, co umożliwia śledzenie statusu weryfikacji wniosku. Po akceptacji prośby przez Facebooka na podany na wcześniejszym etapie adres mailowy wysłany jest token. Za jego pomocą można uzyskać dostęp do żądanych danych, przy czym usługodawca może udostępnić jedynie część wnioskowanych danych, wedle własnego uznania[76].

Jak wynika z informacji uzyskanych od respondentów, w przypadku zastosowania pilnego trybu udostępnienia informacji w sytuacji bezpośredniego zagrożenia życia Facebook udzielił informacji niezwłocznie, a nadto zakresem wydanych danych objął treść prywatnej korespondencji osoby[77]. Relacje funkcjonariuszy Policji w toku prowadzonych badań potwierdzają zasady opisane w wytycznych dotyczących udostępniania danych.

Niestety w żadnym z omawianych trybów nie można, według relacji tych badanych, którzy udzielili na ten temat informacji, uzyskać danych usuniętych przez użytkownika[78]. Jak wspomniano w części dotyczącej przetwarzania danych przez portale społecznościowe, samo usunięcie treści przez użytkownika nie oznacza, że jest ona niedostępna dla usługodawcy, który przez określony czas te dane przetwarza. Niemniej usunięcie treści powoduje, że w omawianym trybie informacja nie zostanie udostępniona. Mając na uwadze powyższe, w przypadku wykrycia podejrzanych treści należy w pierwszej kolejności złożyć wniosek o zabezpieczenie danych, a następnie o ich udostępnienie.

Globalne firmy technologiczne publikują tzw. raporty przejrzystości, w których zamieszczają między innymi dane o liczbie składanych przez właściwe organy wniosków o udostępnienie informacji[79]. Ostatni raport Facebooka, dotyczący okresu od lipca do grudnia 2018 roku, podaje dane dotyczące wszystkich wniosków o udostępnienie informacji pochodzących z Polski, zatem nie tylko wniosków Policji, lecz także sądów, w tym w sprawach innych niż karne[80]. Według raportu łącznie złożono 1912 wniosków o udostępnienie informacji, z czego 1724 wnioski procesowe, co stanowi 90,2% wszystkich żądań. Wniosków awaryjnych złożono odpowiednio 188, co stanowi 9,8% cało-

---

[76] W zakresie skuteczności składanych wniosków zob. *Facebook Transparency Report – Poland*, op. cit.

[77] Badania własne, zob. przypis nr 1.

[78] Ibidem.

[79] Zob. *Raport przejrzystości Google – raporty innych firm z branży*, https://transparencyreport.google.com/about [dostęp: 4 sierpnia 2019 roku].

[80] *Facebook Transparency Report – Poland*, op. cit.

ści. Procent wszystkich uznanych wniosków, dla których udostępniono dane, wynosi 52%, z czego w przypadku wniosków awaryjnych 83%, wniosków procesowych zaś – 49%. W zakresie wniosków o zabezpieczenie Facebook na 219 złożonych wniosków zabezpieczył dane 384 użytkowników (jeden wniosek może dotyczyć kilku kont). Porównanie obecnej liczby wniosków z pierwszym raportem z roku 2013 wskazuje ich istotny wzrost, stanowiący obecnie ośmiokrotność pierwotnie kierowanych żądań[81].

Twitter

W zakresie udostępniania danych przez Twittera należy zwrócić uwagę, że ten usługodawca nie sformułował jasno w swoim regulaminie zasad dotyczących udostępniania danych dla organów ścigania. Odnośne informacje znajdują się wyłącznie w wyodrębnionych wytycznych, sformułowanych w języku angielskim. Portal wyróżnia dwa rodzaje wniosków: o zachowanie danych, które stanowią potencjalnie istotne dowody, oraz o ich udostępnienie.

Zgodnie z wytycznymi Twittera, opierającymi się na przepisach amerykańskich, każdy wniosek powinien być sporządzony na papierze firmowym, z podpisem uprawnionej osoby, zawierać zwrotny adres mailowy, a także wymieniać nazwę użytkownika i adres URL danej treści na Twitterze lub numer identyfikacyjny konta[82]. W zakresie prośby o udostępnienie danych Twitter uzależnia swoje wymagania od rodzaju danych, o jakie się wnosi. Jeżeli żądanie dotyczy danych niepublicznych użytkownika, to wymagany jest odpowiedni nakaz wydania rzeczy, natomiast treści komunikatów, tweety, wiadomości wysyłane pomiędzy użytkownikami czy zdjęcia wymagają nakazu przeszukania. Co do informacji zawartych we wniosku Twitter również wymaga podania danych identyfikacyjnych, a także szczegółowych informacji na temat związku żądanych danych z toczącym się postępowaniem. Twitter podobnie jak Facebook ma specjalny kanał kontaktu z organami ścigania[83].

Pozyskiwanie danych w ramach współpracy międzynarodowej

Polskie organy ścigania mogą, niezależnie od procedury, o której mowa w poprzedniej części niniejszego artykułu, występować także z żądaniem wydania danych w ramach współpracy międzynarodowej. Biorąc pod uwagę, że postępowanie w sprawie udostępnienia danych na podstawie regulaminów po-

81 Ibidem. Dane porównawcze lipiec-grudzień 2013 (220 wniosków łącznie) oraz lipiec-grudzień 2018 (1912 wniosków łącznie).

82 *Guidelines for law enforcement*, online: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support [dostęp: 4 sierpnia 2019 roku].

83 Zob. *Legal request submissions*, https://legalrequests.twitter.com/forms/landing_disclaimer [dostęp: 4.08.2019].

szczególnych usługodawców jest fakultatywne i organy ścigania mogą otrzymać odmowę wydania żądanych danych, niezbędne może być nawiązanie współpracy z organami państwa właściwego usługodawcy. W toku prowadzonych badań nad wykorzystaniem mediów społecznościowych w pracy organów ścigania respondenci, określając możliwe sposoby uzyskiwania danych, wskazywali na potencjalną drogę skorzystania z międzynarodowej pomocy prawnej we współpracy ze Stanami Zjednoczonymi[84]. Jak jednak wspomniano wcześniej, administratorami danych osobowych użytkowników pochodzących z terytorium Europy są spółki z siedzibą w Irlandii. Po ustaleniu danych konta można skorzystać z instrumentów międzynarodowych regulujących współpracę pomiędzy państwami członkowskimi, przy czym należy przyjąć, że taka okoliczność z zasady będzie mieć zastosowanie w przypadku polskich użytkowników mediów społecznościowych. Funkcjonariusze polskich organów ścigania w niektórych, pojedynczych przypadkach błędnie utożsamiali żądanie udostępnienia informacji z koniecznością zwracania się z pomocą prawną do Stanów Zjednoczonych. Ponadto w części przypadków nie podejmowali oni żadnej próby nawiązania oficjalnego kontaktu z usługodawcą, argumentując to zasłyszanymi historiami o negatywnych doświadczeniach z tego typu działaniami z innych jednostek[85]. Należy jednak podkreślić, że zarówno operatorzy mediów społecznościowych, prawo międzynarodowe, jak i polskie przepisy zapewniają możliwość zdobycia pożądanych informacji. W każdym przypadku należy wziąć jednak pod uwagę względy proporcjonalności oraz ekonomiki procesowej. Wykorzystanie narzędzi międzynarodowej pomocy prawnej może być bowiem w pewnych sytuacjach niezasadne.

Uznając, że siedziby portali społecznościowych znajdujących się w kręgu zainteresowania niniejszego artykułu mieszczą się w Irlandii, artykuł skupia się na odmiennościach i specyfice współpracy w zakresie uzyskiwania dowodów wyłącznie z tym państwem.

Podstawami prawnymi właściwymi współpracy sądowej państw członkowskich Unii Europejskiej są art. 82–86 TFUE[86], które tworzą podstawę dla prawa pochodnego UE, regulującego szczegółowo zagadnienia współpracy w sprawach cywilnych i karnych. W zakresie uzyskiwania dowodów na terenie Unii Europejskiej doniosłym praktycznie aktem prawnym jest dyrektywa w sprawie europejskiego nakazu dochodzeniowego[87], która jednak nie ma za-

[84] Badania własne, zob. przypis nr 1.

[85] Badania własne, zob. przypis nr 11.

[86] Traktat o funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz.U. 2004 Nr 90, poz. 864, ze zm.).

[87] Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (OJ L 130, 1.5.2014, p. 1–36).

stosowania w przypadku dwóch państw członkowskich, w tym właśnie Irlandii[88]. Wyłączenie zastosowania przepisów wspomnianej dyrektywy powoduje konieczność oparcia współpracy międzynarodowej na starszych i mniej efektywnych narzędziach, tj. decyzji w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych[89], która od 18 grudnia 2020 roku zostanie zastąpiona rozporządzeniem w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty[90]. Nowe rozporządzenie jednak także nie ma zastosowania do Irlandii[91], stąd nawet po 2020 roku państwa członkowskie w sprawach karnych w relacjach z Irlandią będą musiały polegać na wspomnianej decyzji, zgodnie z którą państwo członkowskie ma uznawać i stosować na swoim terytorium postanowienie o zabezpieczeniu wydane przez organ sądowy innego państwa członkowskiego. Przedmiotowa zasada wzajemnego uznawania nie została jednak w pełni zrealizowana z uwagi na brak pełnego automatyzmu wykonywania orzeczeń w innym państwie członkowskim Unii Europejskiej. Wydane w Polsce orzeczenie nie skutkuje zabezpieczeniem dowodów w innym państwie, lecz podlega wykonaniu poprzez decyzję państwa wykonującego[92]. Zatem w świetle ekonomiki procesowej oraz zasady szybkości postępowania organy ścigania powinny w pierwszej kolejności występować z żądaniem udostępnienia informacji na podstawie regulaminów usługodawców, natomiast dopiero w razie odmowy udostępnienia danych należy stosować procedury współpracy międzynarodowej. Praktyka Facebooka odnosząca się do udostępniania danych wskazuje, że w przypadku wątpliwości co do żądania wniesionego przez organy ścigania za pośrednictwem strony tego usługodawcy odmowa udostępnienia informacji jest uzupełniana stwierdzeniem, że dane mimo wszystko mogą zostać udostępnione, pod warunkiem zachowania właściwej procedury wynikającej z irlandzkich przepisów[93].

---

[88] Zgodnie z art. 1 i 2 oraz art. 4a ust. 1 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który jest dołączony do TUE (Traktatu o Unii Europejskiej) oraz TFUE, Irlandia nie uczestniczy w przyjęciu dyrektywy, nie jest nią związana ani jej nie stosuje.

[89] Decyzja ramowa Rady 2003/577/WSiSW z dnia 22 lipca 2003 r. w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych (OJ L 196, 2.8.2003, p. 45–55), dalej zwana „Decyzją".

[90] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1805 z dnia 14 listopada 2018 r. w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty (OJ L 303, 28.11.2018, p. 1–38).

[91] Zob. przypis nr 88.

[92] P. Kołodziejski, *Kradzieże samochodów i instrumenty prawne współpracy międzynarodowej w tych sprawach*, „Prokuratura i Prawo" 2012, nr 3, s. 3, zob. także G. Jaworski, O. Sołtysińska, *Postępowanie w sprawach karnych ze stosunków międzynarodowych. Komentarz*, Wolters Kluwer Polska, Warszawa 2010, s. 82.

[93] Zob. *Facebook Ireland Ltd. Report of audit*, Irish Data Protection Commisioner, December

W świetle Decyzji procedura jest dwustopniowa i w pierwszej kolejności polega na zabezpieczeniu dowodów, następnie zaś – na ich wydaniu. Postępowanie w sprawie zabezpieczenia dowodów w innym państwie członkowskim Unii Europejskiej wynikające z Decyzji zostało uregulowane w polskich przepisach w rozdziale 62a oraz 62b k.p.k., natomiast implementacja w prawie irlandzkim została dokonana w drodze ustawy z 2008 roku o wzajemnej współpracy w sprawach karnych[94].

Zgodnie z polskimi przepisami z żądaniem zabezpieczenia dowodów może wystąpić prokurator lub sąd, bezpośrednio do organu sądowego danego państwa. Jednak przed zwróceniem się z żądaniem udzielenia pomocy pierwszym krokiem powinno być wydanie postanowienia o zatrzymaniu rzeczy na podstawie przepisów rozdziału 25 k.p.k. Na tym etapie stosuje się wyłącznie polskie przepisy. Kolejnym krokiem jest rozpoczęcie dwuetapowej procedury zabezpieczenia oraz wydania dowodów. Prokurator lub sąd na podstawie art. 589g § 1 k.p.k. powinien wystąpić (w drodze postanowienia) bezpośrednio do właściwego organu państwa członkowskiego z żądaniem wykonania wcześniej wydanego postanowienia krajowego – z pominięciem pośrednictwa Ministerstwa Sprawiedliwości[95]. Wbrew ogólnej zasadzie wskazanej w Decyzji, orzeczenia nie są w przypadku Irlandii przekazywane między organami sądowymi. Adresatem powinien być tzw. organ centralny, którym jest Minister Sprawiedliwości i Równości (ang. *Minister for Justice and Equality*, irl. *An tAire Dlí agus Cirt agus Comhionannais*)[96]. Wraz z orzeczeniem polski organ procesowy powinien przekazać zaświadczenie, zawierające szczegółowe informacje niezbędne do wykonania wniosku, którego treść określa rozporządzenie Ministra

2011, s. 99, online: https://www.pdpjournals.com/docs/87980.pdf?fbclid=IwAR0FKMKggi91fDgb46zAWZjN0oiTCPDwNcE9qMR_Z7FHvVYYlhSezTR5fKs [dostęp: 30.07.2019].

94 *Criminal Justice (Mutual Assistance) Act 2008*, zob. wersję ujednoliconą – *Criminal Justice (Mutual Assistance) Act 2008 revised*, online: http://revisedacts.lawreform.ie/eli/2008/act/7/revised/en/html [dostęp: 29.07.2019].

95 K.T. Boratyńska, A. Górski, A. Sakowicz, *Kodeks postępowania karnego. Komentarz*, wyd. 5, Warszawa 2014, System Informacji Prawnej Legalis; zob. art. 613 § 1 k.p.k.

96 Mutual Assistance and Extradition Division, Department of Justice, Equality and Law Reform, Pinebrook House, 71-74 Harcourt Street. Dublin 2, Ireland, tel: + 353 1 6028589, 6028535, 6028605, faks: + 353 1 6028606, za: *Notification by Ireland on the implementation of the Framework Decision on Freezing Orders*, online: https://www.ejn-crimjust.europa.eu/ejn/libshowdocument/EN/342/EN [dostęp: 30.07.2019].
Irlandia jako jedno z niewielu państw była uprawniona do wskazania organu centralnego. Należy jednak zauważyć, że wiele państw członkowskich wbrew treści Decyzji postanowiło zrezygnować z zasady bezpośredniego przekazywania orzeczeń pomiędzy organami sądowymi – zob. Implementation of the Framework Decision of the Council of the European Union of 22 July 2003 (2003/577/JHA) on the execution in the European Union of orders freezing property or evidence (14349/16, COPEN 336, EUROJUST 146 EJN 7), online: https://www.ejn-crimjust.europa.eu/ejnupload/Practical_info/FO/ImplementationFO16.PDF [dostęp: 30.07.2019].

Sprawiedliwości[97]. Przekazując do wykonania postanowienie o zatrzymaniu dowodów, właściwy sąd lub prokurator występuje jednocześnie do właściwego organu sądowego państwa wykonania postanowienia z wnioskiem o ich wydanie (art. 589g § 2 k.p.k.). Wyżej wskazane dokumenty przed przekazaniem powinny zostać przetłumaczone na język angielski lub irlandzki. Samo przekazanie nie musi odbywać się w drodze przekazania oryginałów dokumentów. Zgodnie z art. 4 ust. 1 Decyzji czynność powinna nastąpić za pomocą jakiegokolwiek środka zdatnego do pozostawienia pisemnego zapisu. Przepisy irlandzkie pozwalają przy tym na przekazanie ich w jakiejkolwiek postaci pozwalającej na stwierdzenie ich wiarygodności, stąd dopuszczalne są także faksymile dokumentów, tj. na przykład przesłanie ich za pomocą faksu lub maila[98]. Jedynie w przypadku wątpliwości co do kompletności dokumentów lub ich wiarygodności irlandzkie ministerstwo lub sąd mogą zwrócić się do polskiego organu z żądaniem dostarczenia oryginału dokumentu lub ustalenia innego sposobu przekazania ich kopii. Irlandzki minister po otrzymaniu dokumentów powinien zwrócić się do irlandzkiego Sądu Najwyższego (ang. *High Court*, irl. *An Ard-Chúirt*) z wnioskiem o wydanie nakazu uznającego postanowienie polskiego organu. O ile nie sprzeciwia się to podstawowym przepisom prawa irlandzkiego, wydane przez tenże sąd orzeczenie powinno uwzględniać wskazane przez polski organ sposoby zabezpieczenia danego dowodu. Zgodnie z przepisami lokalnymi, instrukcyjny termin rozpoznania wniosku o zabezpieczenie dowodów wynosi 24 godziny od otrzymania postanowienia wraz z zaświadczeniem. Irlandzki Sąd Najwyższy może odmówić lub odroczyć wydanie nakazu w przypadku, gdy: (i) czyn nie stanowi przestępstwa na gruncie prawa międzynarodowego, (ii) przekazane dokumenty są niekompletne, (iii) na gruncie prawa irlandzkiego przysługuje immunitet uniemożliwiający wykonanie zabezpieczenia lub (iv) przekazanie dowodów w związku z przestępstwem naruszyłoby zasadę *ne bis in idem*. Właściwe orzeczenie sądu jest przekazywane podmiotom, których dotyczy. Okres, przez który zabezpiecza ono dowody, wyznacza przekazanie dowodów do Polski lub wydanie odmowy ich przekazania, niemniej orzeczenie może zostać także uchylone przez sam sąd. Irlandzkie przepisy dają organowi stosunkowo dużą swobodę, określając jako możliwą

[97] Rozporządzenie Ministra Sprawiedliwości w sprawie wzoru zaświadczenia stosowanego we współpracy z państwami członkowskimi Unii Europejskiej w zakresie wzajemnego wykonywania orzeczeń o zatrzymaniu dowodów i zabezpieczeniu mienia na poczet przepadku (Dz.U. z 2005 r. Nr 166, poz. 1393)

[98] Zob. *Mutual legal assistance in criminal matters. A guide to Irish law and procedures.,* Department of Justice and Equality, s. 20, online: http://www.justice.ie/en/JELR/Guide_to_Irish_Law_and_Procedures_-_Mutual_legal_Assistance_in_Criminal_Matters.pdf/Files/Guide_to_Irish_Law_and_Procedures_-_Mutual_legal_Assistance_in_Criminal_Matters.pdf [dostęp: 30.07.2019].

podstawę uchylenia np. przypadek, w którym sąd uzna, że z jakiegokolwiek powodu pozostawanie orzeczenia w mocy nie leży w interesie sprawiedliwości. Inicjatywa w tym zakresie leży po stronie zarówno osób dotkniętych postanowieniem, jak i samego sądu. Należy przy tym zaznaczyć, że zgodnie z art. 11 ust. 2 Decyzji merytoryczne podstawy wydania postanowienia mogą być zakwestionowane wyłącznie w państwie wydającym.

Drugim etapem jest przekazanie zabezpieczonych dowodów do Polski. Zgodnie z przepisami irlandzkimi postanowienie o wydaniu dowodów, przekazane razem z zaświadczeniem i postanowieniem o zabezpieczeniu dowodów, powinno być traktowane jak wniosek o pomoc prawną w uzyskaniu dowodów, z tym zastrzeżeniem, że sąd nie może odmówić przekazania dowodów, jeżeli mają być one wykorzystane w postępowaniu dotyczącym przestępstwa wymienionego w art. 3 ust. 2 Decyzji, które zagrożone jest w Polsce karą co najmniej 3 lat pozbawienia wolności[99]. Z zastrzeżeniem powyższego przekazanie dowodów nie będzie możliwe w ramach omawianej procedury, gdy przestępstwo zagrożone jest w Irlandii lub Polsce karą łagodniejszą niż sześć miesięcy pozbawienia wolności. Niestety etap ten odbywa się na zasadach międzynarodowej pomocy prawnej, określonych Konwencją o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej[100]. W związku z tym, że Irlandia wskazała na swoim terytorium jako organ właściwy tzw. organ centralny, do zwracania się o pomoc prawną wyłącznie właściwa jest prokuratura krajowa[101]. Powyższe sprawia, że procedura uzyskiwania dowodów z mediów społecznościowych za pośrednictwem innych kanałów komunikacji niż zasady określone przez usługodawców jest bardziej złożona pod względem proceduralnym.

Podsumowanie

Tematyka pozyskiwania danych z mediów społecznościowych jest niewątpliwie istotna z punktu widzenia praktyki działania organów ścigania. Jakkolwiek przedstawione w artykule informacje odnosiły się wyłącznie do pozy-

[99] Spośród przestępstw, w odniesieniu do których policjanci najczęściej wykorzystywali dane pochodzące z Facebooka (badanie własne – zob. przypis nr 11) niniejsze przepisy stawiają pod znakiem zapytania skuteczność występowania z wnioskiem do Irlandii w sprawach przestępstw z art. 212, 216 oraz 256 k.k.

[100] Konwencja ustanowiona przez Radę zgodnie z art. 34 Traktatu o Unii Europejskiej o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (OJ C 197, 12.7.2000, p. 3–23); zob. art. 10 ust. 2 Decyzji.

[101] C. Kłos, *Pomoc prawna, wybrane zagadnienia* w: J. Gemra (red.), *Metodyka pracy w sprawach karnych ze stosunków międzynarodowych*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 18.

skiwania danych, nie zaś do dalszych etapów, takich jak np. ich wprowadzanie do procesu karnego, to pokazują one zarys ram funkcjonowania tzw. dowodów z Facebooka, jak określali je badani funkcjonariusze Policji[102]. Należy zwrócić uwagę, że przeprowadzone badania miały charakter eksploracyjny, stąd niezbędna jest ich kontynuacja. Dotychczas nie podjęto w Polsce kompleksowych badań naukowych dotyczących korzystania z mediów społecznościowych przez funkcjonariuszy Policji, problematyka ta nie była także przedmiotem szerszej debaty. Niemniej zarówno środowisko naukowe, jak i organy ścigania powinny pogłębiać wiedzę dotyczącą wykorzystania mediów społecznościowych. Szczególną uwagę należy zwrócić na problematykę zabezpieczania dowodów pochodzących z *social media* oraz ich wartości w procesie karnym, przede wszystkim z uwagi na stale zwiększającą się liczbę użytkowników mediów społecznościowych opisywanych w niniejszym artykule[103], a także powstawanie nowych portali, np. TikTok, którego głównymi użytkownikami są dzieci[104].

Ze względu na coraz większą cyfryzację życia niewątpliwie wzrastać będzie znaczenie dowodów cyfrowych w procesie karnym. Jako że ich pozyskiwanie często wiąże się z elementem transgranicznym, tj. niezbędne jest wystąpienie z żądaniem do państwa obcego, potrzebna jest współpraca na szczeblu międzynarodowym, która ułatwi udostępnianie dowodów cyfrowych[105]. W tym zakresie należy rozważyć możliwość nawiązania bezpośredniej, bilateralnej współpracy z państwami, w których znajdują się siedziby usługodawców.

Niezależnie od powyższego konieczne jest także podjęcie w kraju takich działań, które spowodują, że wykorzystanie mediów społecznościowych, wiedza praktyczna i prawna w tym zakresie, stanie się podstawowym elementem

[102] W ten sposób badani funkcjonariusze Policji zbiorczo określali dowody pochodzące z mediów społecznościowych, w zakresie badań zob. przypis nr 11.

[103] P. Rosa, *Social media*, op. cit.; *Facebook reports fourth quarter and full year 2018 results*, op. cit.

[104] 65% badanych polskich użytkowników aplikacji TikTok stanowią osoby w wieku od 13 do 15 lat, drugą najliczniejszą grupą są osoby w wieku poniżej 13 lat (18%). Ogólna liczba aktywnych użytkowników miesięcznie na świecie to około 500 milionów osób. Zob. *Kim są polscy użytkownicy TokTok*, styczeń 2019, online: https://www.gethero.pl/raport-tiktok/ [dostęp: 7.08.2019].

[105] Zob. inicjatywę uregulowania współpracy UE–USA: *Addendum to the Recommendation for a Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, online: https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/en/pdf [dostęp: 1.08.2019] oraz amerykańską ustawę, tzw. *Cloud Act*, stwarzającą możliwość nawiązania bezpośredniej współpracy bilateralnej, w wyniku której państwa trzecie mogą bezpośrednio kierować żądania udostępnienia danych do amerykańskich usługodawców, bez wymogu wydawania właściwych orzeczeń przez organy amerykańskie, zob. *Cloud Act Resoruces*, online: https://www.justice.gov/dag/cloudact [dostęp: 4.08.2019].

szkolenia funkcjonariuszy Policji i prokuratorów. Autorzy postulują, oprócz modyfikacji programów szkoleniowych, wydanie przez Komendanta Głównego Policji wytycznych, które wskażą metodykę postępowania funkcjonariuszy w przypadku konieczności pozyskania dowodów oraz informacji za pośrednictwem mediów społecznościowych. Powinny one określać sposób korzystania z *social media*, w szczególności w zakresie wykorzystywania konta zarejestrowanego na dane fałszywe, dokumentowania podejmowanych czynności, a także współpracy z prokuraturą w przypadku podejmowania czynności niebędących czynnościami operacyjno-rozpoznawczymi, wymagającymi nawiązania kontaktu z danym usługodawcą. Przedmiotowe wytyczne ujednoliciłyby dotychczasową praktykę organów ścigania, która w świetle badań[106] jest różnicowana. Obecny stan, w którym funkcjonariusze Policji muszą samodzielnie zdobywać wiedzę w omawianym zakresie, nie sprzyja korzystaniu przez nich z mediów społecznościowych w postępowaniu karnym[107].

Streszczenie

Artykuł porusza problematykę pozyskiwania przez polskie organy ścigania danych z Facebooka, Twittera oraz Instagrama, zarówno w drodze bezpośredniego kontaktu z danym usługodawcą, z wykorzystaniem instrumentów międzynarodowej pomocy prawnej, jak i w drodze czynności operacyjno-rozpoznawczych. Zakres artykułu został zawężony do pozyskiwania danych pochodzących z terenu Unii Europejskiej. Autorzy opisują podstawy prawne przetwarzania danych osobowych przez usługodawców, dokonywania przez funkcjonariuszy Policji czynności białowywiadowczych w mediach społecznościowych, proces pozyskiwania danych z *social media* na podstawie regulaminów wewnętrznych usługodawców, a także przepisy polskie, unijne oraz irlandzkie.

Autorzy sygnalizują potrzebę prowadzenia dalszych badań w zakresie wykorzystania mediów społecznościowych w pracy organów ścigania, wydanie przez Komendanta Głównego Policji wytycznych co do sposobu sięgania do mediów społecznościowych, a także przeprowadzenie odpowiednich szkoleń dla funkcjonariuszy. Ponadto artykuł zwraca uwagę na złożony proceduralnie proces pozyskiwania danych od usługodawców z wykorzystaniem instrumentów międzynarodowej pomocy prawnej. Autorzy postulują w tym zakresie rozważenie zawarcia przez Polskę odpowiednich umów bilateralnych z państwami, w których swoje siedziby mają usługodawcy, opartych na wskazanych w artykule dostępnych rozwiązaniach prawnych.

Słowa kluczowe: media społecznościowe, biały wywiad, Policja, dane, międzynarodowa pomoc prawna

---

[106] Badania własne, zob. przypis nr 1.

[107] Zob. K. Bayer, J. Bitner, *Wykorzystanie mediów społecznościowych w pracy polskiej Policji. Próba wstępnej analizy na podstawie wyników badań kwestionariuszowych* (w druku); M. Czekalska, K. Krawczyk, *Wykorzystanie informacji z mediów społecznościowych (SOCMINT) jako narzędzie pracy polskiej Policji (wyniki badań ankietowych)* (w druku).

Summary

The article raises the issue of data acquisition from Facebook, Twitter and Instagram by the Polish law enforcement, both through direct contact with the service provider, using the instruments of international legal assistance, and investigative operations. The authors refers both to the internal regulations of service providers, Polish, EU and foreign legislation. Scope of the article has been narrowed down to the acquisition of data collected in the European Union. The authors describe the legal bases for processing personal data by service providers, conducting OSINT activities in social media by police officers, the process of obtaining data from social media based on the terms of service providers, as well as Polish, EU and Irish laws.

The authors point out the necessity of conducting further research on the use of social media by law enforcement agencies, to publish by the Police General Commandant guidelines on the use of social media and to conduct appropriate training for officers. Moreover, the article draws attention to the procedurally complex process of obtaining data from service providers with use of international legal assistance instruments. Therefore, the authors propose that Polish government should consider concluding appropriate bilateral agreements, on the basis of already available legal solutions indicated in the article, with countries where service providers are established.

Keywords: social media, OSINT, Police, data, international legal assistance

Bibliografia

Literatura

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, wyd. 4, Warszawa 2016, System Informacji Prawnej Legalis.

Baser D., *Hard questions: What data does Facebook collect when I'm not using Facebook, and why?*, Facebook Newsroom, kwiecień 2018, online: https://newsroom.fb.com/news/2018/04/data-off-facebook/ [dostęp: 4.08.2019].

Bayer K., Bitner J., *Wykorzystanie mediów społecznościowych w pracy oolskiej Policji. Próba wstępnej analizy na podstawie wyników badań kwestionariuszowych* (w druku).

Boratyńska K.T., Górski A., Sakowicz A., *Kodeks postępowania karnego. Komentarz*, wyd. 5, Warszawa 2014, System Informacji Prawnej Legalis.

Cabañas J.G., Cuevas Á., Cuevas R., *Unveiling and quantifying Facebook exploitation of sensitive personal data for advertising purposes*, 2018, online: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-cabanas.pdf [dostęp: 28.07.2019].

Chałubińska-Jentkiewicz K., Taczkowska-Olszewska J., *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, System Informacji Prawnej Legalis.

Cunche M., *I know your MAC Address: Targeted tracking of individual using Wi-Fi*, online: https://hal.inria.fr/file/index/docid/858324/filename/Wi-Fi_Stalking.pdf [dostęp: 6.08.2019].

Czekalska M., Krawczyk K., *Wykorzystanie informacji z mediów społecznościowych (SOCMINT) jako narzędzie pracy polskiej Policji (wyniki badań ankietowych)* (w druku).

Fołta T., Mucha A., *Zniesławienie i znieważenie w internecie*, „Prokuratura i Prawo" 2006, nr 11.

Golański A., *Sukces Microsoftu w walce z wujem Samem: serwery w Europie poza jurysdykcją USA*, lipiec 2016, online: https://www.dobreprogramy.pl/Sukces-Microsoftu-w-walce-z-wujem-Samem-serwery-w-Europie-poza-jurysdykcja-USA,News,74797.html [dostęp: 4.08.2019].

Grzegorczyk T., Tylman J., *Polskie postępowania karne*, wyd. IX, Wolters Kluwer, Warszawa 2014.

Hanausek T., *Kryminalistyka. Zarys wykładu*, Zakamycze, Kraków 1996.

Ingram D., *Facebook to put 1.5bn users out of reach of new EU GDPR privacy law*, „The Irish Times", kwiecień 2018, online: https://www.irishtimes.com/business/technology/facebook-to-put-1-5bn-users-out-of-reach-of-new-eu-gdpr-privacy-law-1.3466837 [dostęp: 4.08.2019].

Jaworski G., Sołtysińska O., *Postępowanie w sprawach karnych ze stosunków międzynarodowych. Komentarz*, Wolters Kluwer Polska, Warszawa 2010.

Kasprzak W., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015.

Klein A., Pinkas B., *DNS cache-based user tracking*, online: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-4_Klein_paper.pdf [dostęp: 6.08.2019].

Kłos C., *Pomoc prawna, wybrane zagadnienia*, w: J. Gemra (red.), *Metodyka pracy w sprawach karnych ze stosunków międzynarodowych*, Wydawnictwo C.H. Beck, Warszawa 2013.

Kołodziejski P., *Kradzieże samochodów i instrumenty prawne współpracy międzynarodowej w tych sprawach*, „Prokuratura i Prawo" 2012, nr 3.

Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011.

Litwiński P., Barta P., Kawecki M., *Artykuł 6 RODO*, w: P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, System Informacji Prawnej Legalis.

McKenna B., *EU regulation set to advance single market for non-personal data*, „Computer Weekly", listopad 2018, online: https://www.computerweekly.com/news/252452332/EU-regulation-set-to-advance-single-market-for-non-personal-data [dostęp: 4.08.2019].

Mroziewicz K., *Czas pluskiew*, Wydawnictwo Sensacje XX Wieku Bogusław Wołoszański, Warszawa 2007, za: K. Jarczewska-Walendziak, *Wykorzystywanie otwartych źródeł informacji przez służby śledcze*, „Toruńskie Studia Bibliologiczne" 2017, nr 1 (18).

Pogorzelski J., *Wykorzystanie otwartych źródeł informacji w pracy prokuratora*, w: W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Wydawnictwo C.H. Beck, Warszawa 2012.

Rogacka-Rzewnicka M., Girdwoyń P., *Undercover Operation, Rapports Polonais XIXth International Congress Of Comparative Law Vienne 20–26 VII 2014*, Łódź 2014.

Rosa P., *Social media*, w: *Raport strategiczny. Internet 2018/2019*, IAB Polska, online: https://iab.org.pl/wp-content/uploads/2019/06/HBRP-raport-IAB-05-191.pdf [dostęp: 22.07.2019].

Sawka N., *Ile jest przestępstw z nienawiści? Czy oficjalne dane są zaniżone?*, styczeń 2019, online: http://sonar.wyborcza.pl/sonar/7,156422,24374999,jak-mowa-nienawisci-staje-sie-elementem-naszej-codziennosci.html?disableRedirects=true [dostęp: 4.08.2019].

Stromczyński B., Waszkiewicz P., *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5.

Źródła i Internet

18 U.S. Code § 2703. Required disclosure of customer communications or records, online: https://www.law.cornell.edu/uscode/text/18/2703 [dostęp: 4.08.2019].

Addendum to the Recommendation for a Council Decisionauthorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, online: https://data.consilium.europa.eu/doc/document/ ST-9666-2019-INIT/en/pdf [dostęp: 1.08.2019].

Agreement on the European Economic Area, https://www.efta.int/sites/default/files/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf [dostęp: 6.08.2019].

Cloud Act Resources, online: https://www.justice.gov/dag/cloudact [dostęp: 4.08.2019].

Criminal Justice (Mutual Assistance) Act 2008 revised, online: http://revisedacts.lawreform.ie/eli/2008/act/7/revised/en/html [dostęp: 29.07.2019].

Decyzja Komendanta Głównego Policji nr 354 z dnia 13 listopada 2015 r. w sprawie programu nauczania na kursie specjalistycznym z analizy kryminalnej w zakresie cyberprzestępczości.

Decyzja nr 322 Komendanta Głównego Policji z dnia 24 października 2018 r. w sprawie programu nauczania na kursie specjalistycznym w zakresie uzyskiwania informacji z Internetu dla Policjantów zwalczających przestępczość komputerową.

Decyzja ramowa Rady 2003/577/WSiSW z dnia 22 lipca 2003 r. w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych (OJ L 196, 2.8.2003, p. 45–55).

Digital 2019 Poland. All the data and trends you need to understand internet, social media, mobile and e-commerce behaviors in 2019, online: https://datareportal.com/reports/digital-2019-poland [dostęp: 4.08.2019].

Digital 2019. Essential insights into how people around the world use the internet, mobile devices, social media, and e-commerce, online: https://wearesocial.com/global-digital-report-2019 [dostęp: 22.07.2019].

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (OJ L 201, 31.7.2002, p. 37–47).

Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (OJ L 130, 1.5.2014, p. 1–36).

Facebook Ireland Ltd. Report of audit, Irish Data Protection Commisioner, December 2011, online: https://www.pdpjournals.com/docs/87980.pdf?fbclid=IwAR0FKMKggi91fDgb46zAWZjN0oiTCPDwNcE9qMR_Z7FHvVYYlhSezTR5fKs [dostęp: 30.07.2019].

Facebook Law Enforcement Guidelines, https://info.publicintelligence.net/Facebook2010-2.pdf [dostęp: 29.07.2019].

Facebook Reports Fourth Quarter and Full Year 2018 Results, online: https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Release.pdf [dostęp: 3.08.2019].

Facebook Transparency Report – Poland, online: https://transparency.facebook.com/government-data-requests/country/PL [dostęp: 4.08.2019].

FBI (2015–2017) Internet Crime Report za: M. McGuire, *Social media platforms and the cybercrime economy*, online: https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf [dostęp: 4.08.2019].

Guidelines for law enforcement, online: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support [dostęp: 4.08.2019].

Implementation of the Framework Decision of the Council of the European Union of 22 July 2003 (2003/577/JHA) on the execution in the European Union of orders freezing property or evidence (14349/16, COPEN 336, EUROJUST 146 EJN 7), online: https://www.ejn-crimjust.europa.eu/ejnupload/Practical_info/FO/ImplementationFO16.PDF [dostęp: 30.07.2019].

Informacje dla organów ścigania, online: https://www.facebook.com/safety/groups/law/guidelines/ [dostęp: 4.08.2019].

Kim są polscy użytkownicy TokTok, styczeń 2019, online: https://www.gethero.pl/raport-tiktok/ [dostęp: 7.08.2019].

Konwencja ustanowiona przez Radę zgodnie z art. 34 Traktatu o Unii Europejskiej o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (OJ C 197, 12.7.2000, p. 3–23).

Law Enforcement Online Requests, online: https://www.facebook.com/records/login/ [dostęp: 4.08.2019].

Legal request submissions, https://legalrequests.twitter.com/forms/landing_disclaimer [dostęp: 4.08.2019].

Mutual legal assistance in criminal matters. A guide to Irish law and procedures, Department of Justice and Equality, online: http://www.justice.ie/en/JELR/Guide_to_Irish_Law_and_Procedures__Mutual_legal_Assistance_in_Criminal_Matters.pdf/Files/Guide_to_Irish_Law_and_Procedures__Mutual_legal_Assistance_in_Criminal_Matters.pdf [dostęp: 30.07.2019].

Notification by Ireland on the implementation of the Framework Decision on Freezing Orders, online: https://www.ejn-crimjust.europa.eu/ejn/libshowdocument/EN/342/EN [dostęp: 30.07.2019].

Polski internet w grudniu 2018, Raport Gemius/PBI, online: http://pbi.org.pl/badanie-gemius-pbi/polski-internet-w-grudniu-2018/ [dostęp: 3.08.2019].

Projekt ustawy o czynnościach operacyjno-rozpoznawczych, online: http://orka.sejm.gov.pl/proc6.nsf/projekty/353_p.htm [dostęp: 29.07.2019].

Raport przejrzystości Google – raporty innych firm z branży, https://transparency-report.google.com/about [dostęp: 4.08.2019].

Regulamin Facebooka, online: https://pl-pl.facebook.com/legal/terms [dostęp: 29.07.2019].

Rozporządzenie Ministra Sprawiedliwości w sprawie wzoru zaświadczenia stosowanego we współpracy z państwami członkowskimi Unii Europejskiej w zakresie wzajemnego wykonywania orzeczeń o zatrzymaniu dowodów i zabezpieczeniu mienia na poczet przepadku (Dz.U. z 2005 r. Nr 166, poz. 1393).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1805 z dnia 14 listopada 2018 r. w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty (OJ L 303, 28.11.2018, p. 1–38).

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) COM(2017) 10 final 2017/0003(COD), online: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010 [dostęp 27.07.2019].

Terms of Service, online: https://twitter.com/tos [dostęp: 4.08.2019].

Traktat o funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz.U. 2004 Nr 90, poz. 864, ze zm.).

Twitter Privacy Policy, online: https://twitter.com/en/privacy [dostęp: 28.07.2019].

Ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (tekst jedn. Dz.U. z 2019 r., poz. 123).

Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz.U. z 2019 r., poz. 53),

Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz.U. z 2018 r., poz. 2387).

Ustawa z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego (tekst jedn. Dz.U. z 2018 r., poz. 1987, ze zm.).

Ustawa z dnia 6 kwietnia 1990 roku o Policji (tekst jedn. Dz.U. z 2019 r., poz. 161).

Ustawa z dnia 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz.U. 2018, poz. 2104).

What is an API?, online: https://www.mulesoft.com/resources/api/what-is-an-api [dostęp: 4.08.2019].

Zasady dotyczące danych Facebooka, online: https://www.facebook.com/policy.php [dostęp: 28.07.2019].

Zasady Twittera, online: https://help.twitter.com/pl/rules-and-policies/twitter-rules [dostęp: 29.07.2019].